Regional Cyber Resiliency

Presented to:

RCPGP National Conference

September 18, 2012

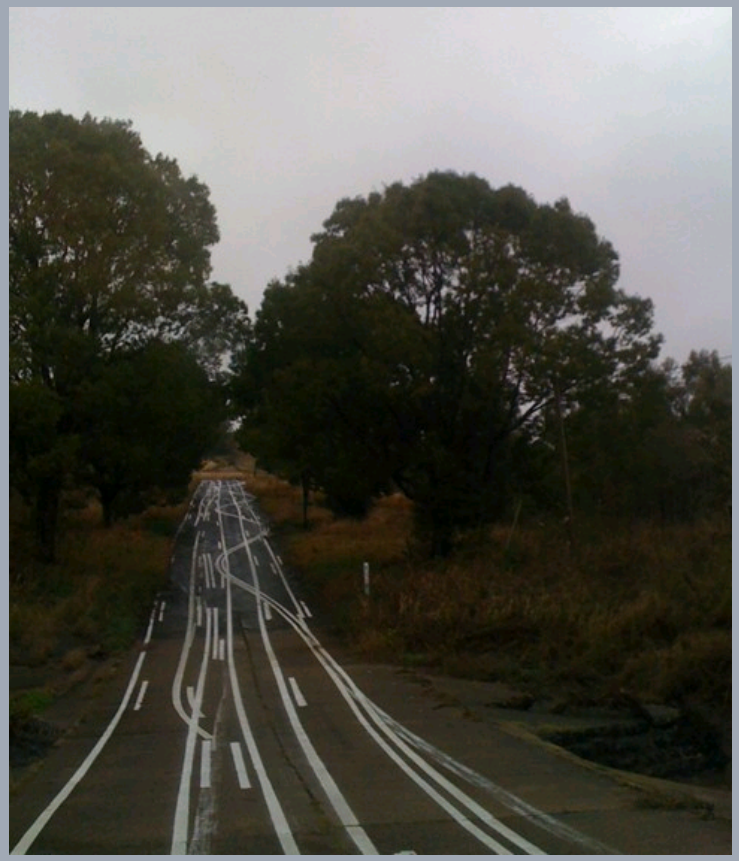
NEW ENGLAND
REGIONAL CATASTROPHIC
PREPAREDNESS INITIATIVE

Session Agenda

- Why Cyber?
- Rhode Island Cyber Disruption Team: *Preparing for Today and tomorrow*
- *Experiences & Challenges*

NERCPI

Cyber Disruption Planning



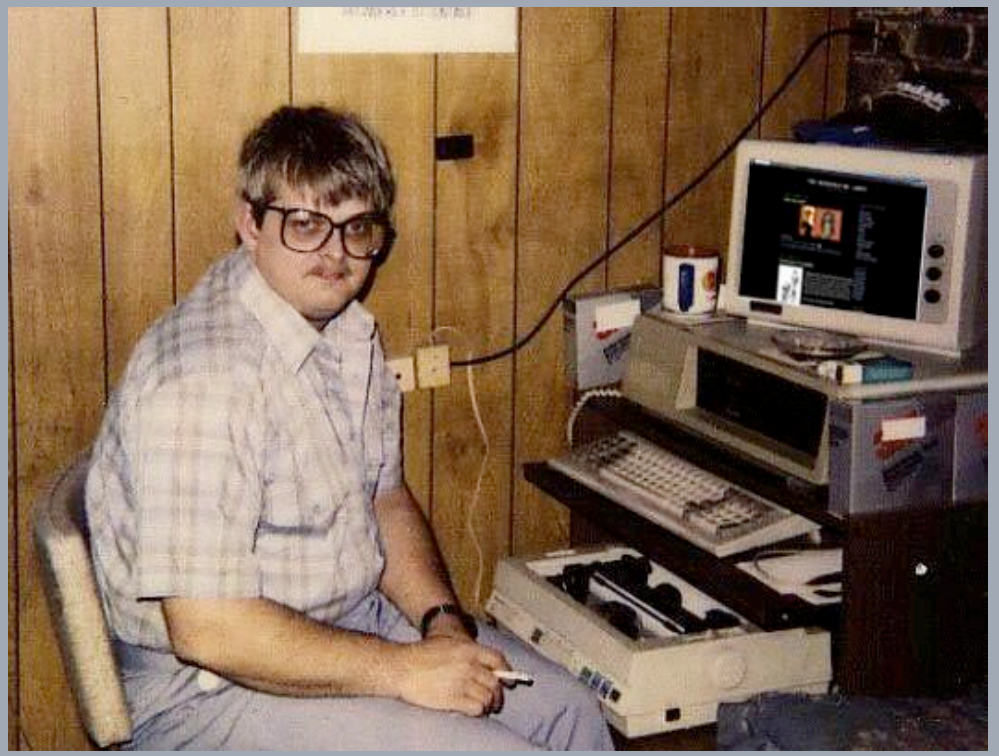
NERCPI

Cyber Disruption Planning

- Catastrophic cyber planning is an evolving concept
- Approach limits risk by maintaining focus on the impact(s) of a given disruption:
  - Loss of Internet
  - Loss of internal network resources
  - Loss of desktop assets
  - Loss of power
  - Loss of physical access to assets

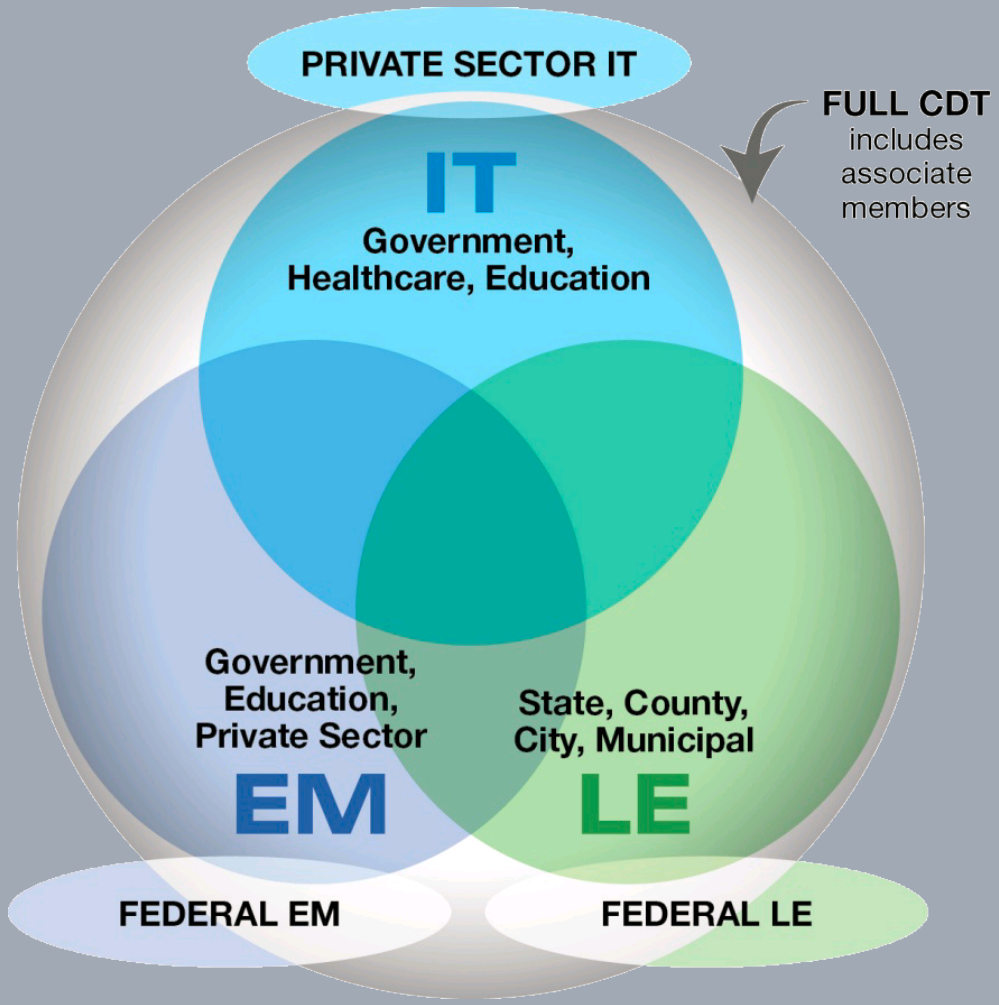
NERCPI

Why does Cyber matter to EM?



Why does Cyber matter to EM?

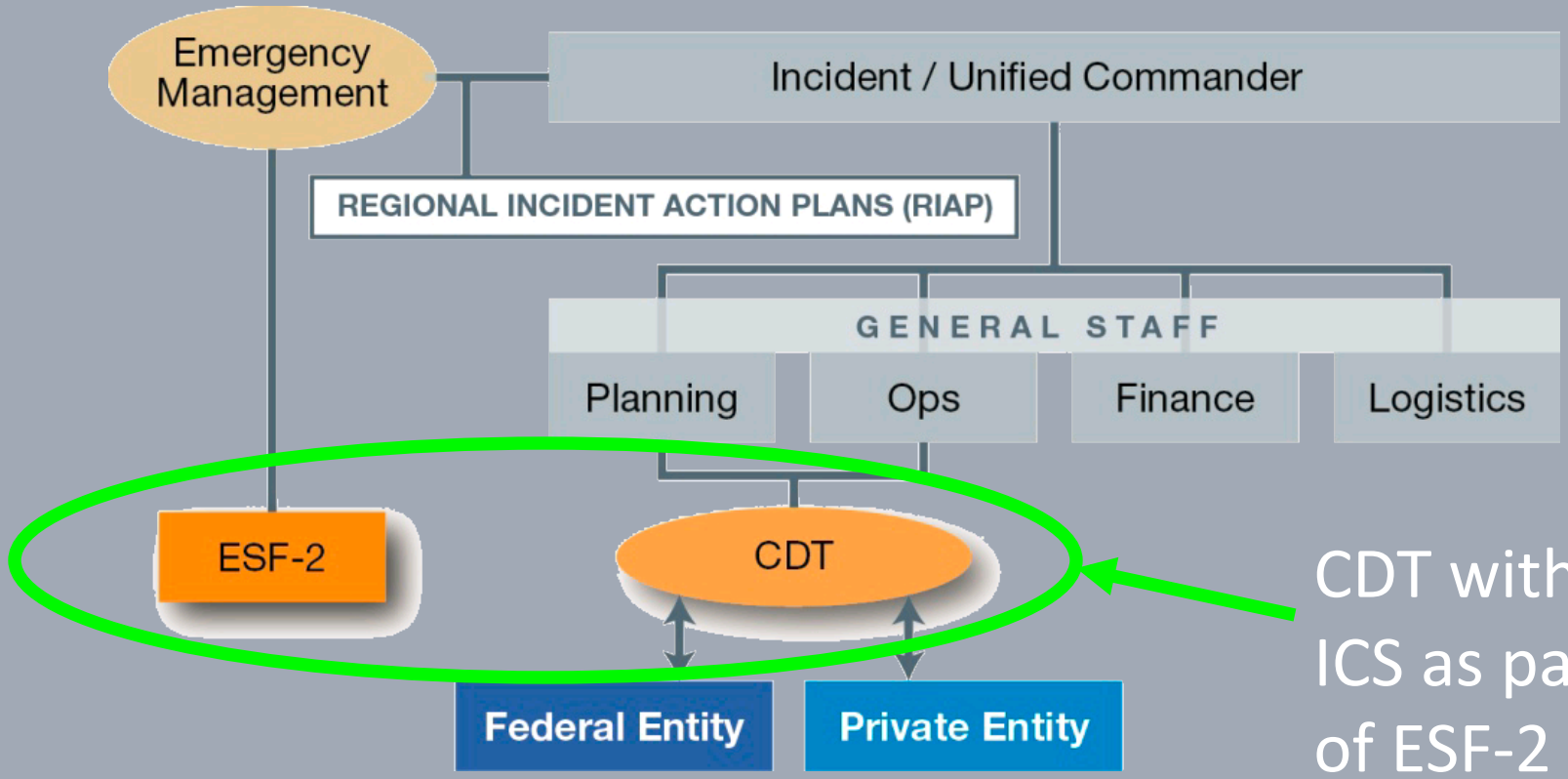
Cyber Disruption Team



The ***CDT*** is the cadre of experts available to manage or assist the management of a critical incident.

NERCPI

Cyber Disruption Team



CDT within ICS as part of ESF-2

NERCPI

Benefits of Collaboration

- Collaboration between EM and IT
  - Better understanding by EM of their reliance on IT systems
  - Breaking down language barriers between IT and EM communities
- IT response can benefit from implementing EM response "battle rhythm"

NERCPI

Lessons Learned

- Interdependencies across utility sectors
- Shows importance of departmental IT disaster recovery
- Prioritization is key for structured restoration
- Span of control differs between EM and IT
  - EM/Public Safety cover entire state assets
  - IT covers executive branch assets

NERCPI

Lessons Learned

- Evidence collection underscores need for law enforcement Presence
- Regional cooperation for information sharing; resource sharing on the horizon
- Awareness briefings require IT and EM understanding among CDT leads

NERCPI

Rhode Island Cyber Disruption Team

Planning for Today and the Future

Theresa Murray
Executive Director, RIEMA

Robert Fitzpatrick
Regional Catastrophic Planner, RIEMA
Co-Lead, RI CDT

RI CDT Mission

- The mission is to respond to cyber disruptions caused by natural hazard, widespread virus or cyber attack which affect critical infrastructure, whether public or private, to ensure continuity of service and the safety of Rhode Island citizens.

Cyber in Emergency Support Function

- **ESF-2 – COMMUNICATIONS**
  - **Lead: Rhode Island Emergency Management Agency**
    - Coordination with telecommunications and information technology industries
    - Restoration and repair of telecommunications infrastructure
    - ***Protection, restoration, and sustainment of national cyber and information technology resources***
      - Oversight of communications within the Federal incident and response structures

NERCPI

Cyber Incident

- An organized attack
- An uncontrolled exploit, such as a virus or worm which has a widespread impact on public safety.
- A natural disaster with significant cyber consequences.
- Other incidents capable of causing extensive damage to critical infrastructure.
- Inadequate or improper information technology (IT) infrastructure maintenance security, and/or design.

NERCPI

Coordination of Response

- The Rhode Island Cyber Disruption Team acts as the lead agency coordinating the cyber-related response component of a broader emergency situation unless or until the event becomes an incident of national significance.

Partnerships

- Financial Industry
- Higher Education
- Defense Industry
- Health Care Providers
- Emergency Services
- Fusion Center

RHODE ISLAND EMERGENCY MANAGEMENT AGENCY 1996

NERCPI

RI State Fusion Center

Information

Information

Analyze

NERCPI

Information Sharing

RI Cyber Disruption Team

- Network Engineering
- Network Security
- Programming/Scripting
- Network Penetration
- Cisco Certified
- Intrusion Detection Systems (IDS)
- Linux

NERCPI

Partners

- Rhode Island State Police, Computer Crimes Unit
- Rhode Island Emergency Management Agency
- Rhode Island Department of Information Technology
- Rhode Island Division of Public Utilities and Carriers
- Rhode Island State Department of Elementary and Secondary Education

NERCPI

Washington State

Domestic Cyber Integrated Project

Background

14 Feb 2012: Senate Floor Testimony on Cybersecurity Act of 2012

Senator Joe Lieberman: *"I know it is February 14, 2012, but I fear that when it comes to protecting America from cyber-attack it is September 10, 2001, and the question is whether we will confront this existential threat before it happens?"*

- **Recognizing the need for greater unity of effort for cyber security, cyber infrastructure protection and protection of the "wa.gov" domain, Washington state officials initiated a "bottom-up" cybersecurity planning effort in early 2012.**
- **Existing FEMA Emergency Support Function 2 (ESF-2) "Communications" was selected as the platform / forum for cyber planning and response**
- **WA Military Department has joint primary lead for ESF-2**
  - Shared responsibility with Consolidated Technology Services (CTS), Office of the Chief Information Officer (OCIO), Department of Enterprise Services (DES), and the Utilities and Transportation Commission (UTC)
- **#1 State OCIO Action Item : Critical Infrastructure Protection from Cyber attack**
- **WA Military Department established a WA State multi-agency *Domestic Cyber Integrated Project Team* (Cyber IPT) in Feb 2012**

IPT Participants

Cyber Integrated Project Team (IPT)

- Leverages key state agencies involved in cyber planning, response, mitigation with Mil Dept cyber assets (ARNG, ANG, State IT)

Objectives:

#1: Develop a domestic Cyber Planning and Response Concept of Operations (Cyber Continuum) for the Washington National Guard that crosswalks military capabilities with state domestic cyber requirements

#2: Develop a Washington State Cyber Incident Response Plan based on NCIRP

#3: Create a “bottom up”-driven State cyber response planning template (requirements, capabilities, action plan) for others in FEMA Region X and nationally that leverages and completes the “Cyber Center of Excellence” in the Pacific Northwest

OCIO
Office of the Chief Information Officer

WASHINGTON UTC
UTILITIES AND TRANSPORTATION COMMISSION

WASHINGTON STATE PATROL
WSP

Citizens Serving Citizens With Pride & Tradition
Washington Military Department

Washington State Department of
Enterprise Services

TWO SIX TWO
NETWORK WARFARE SQ

W

CTS
Consolidated Technology Services • WA

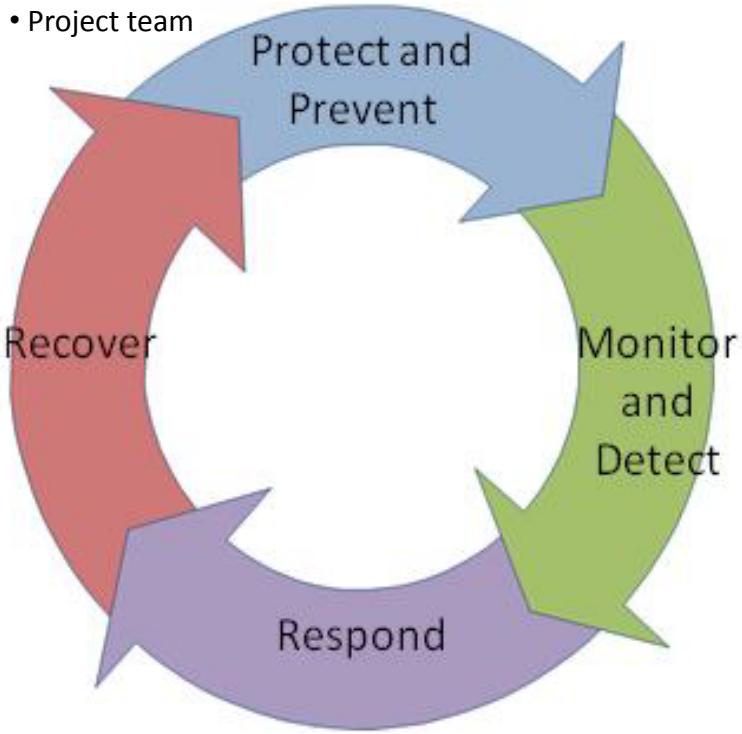
Objective #1: Domestic Cyber Continuum

Potential Mission Assignment Options for National Guard forces

Based on traditional National Cyber Incident Response Plan (NCIRP) Framework

How can the National Guard support the domestic cyber continuum?

- System Security standard consultation
- Compliance reviews
- Exercise support
- Project team



- Vulnerability Identification and Remediation

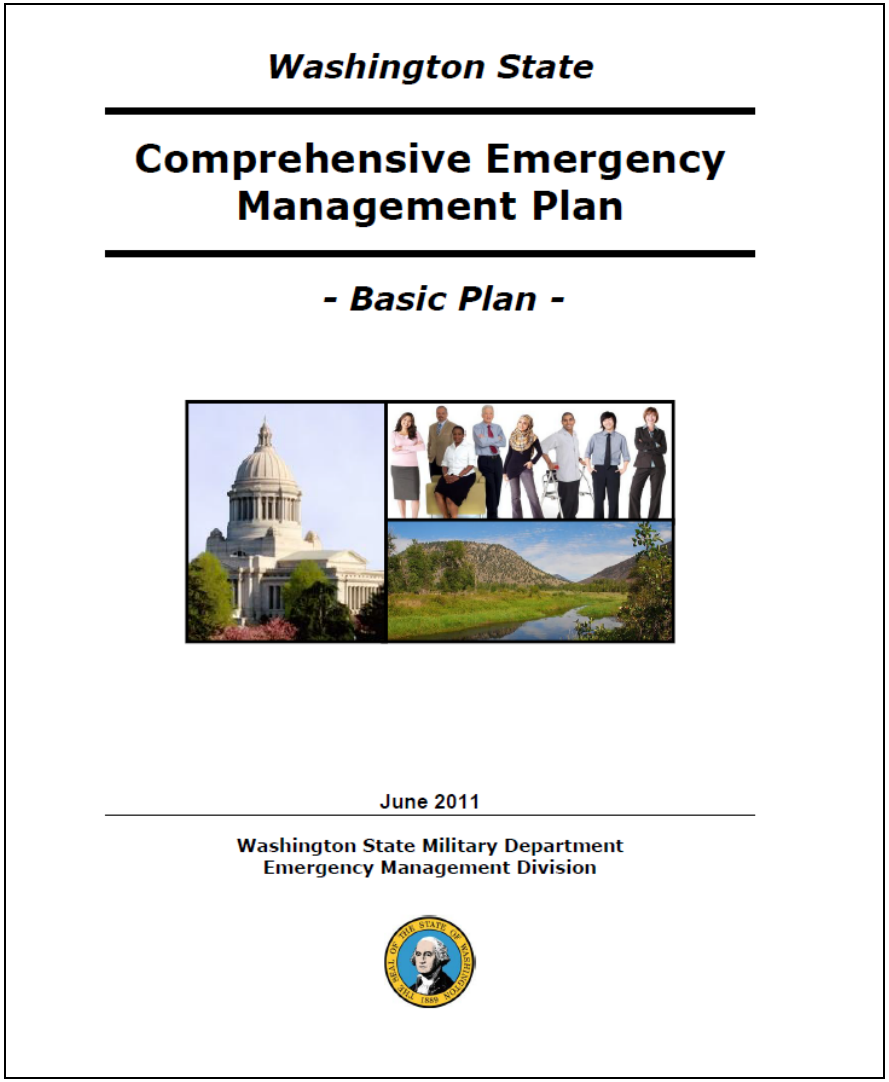
- Law Enforcement Support
- Incident Response Teams
- Forensics
- Root Cause
- Attribution

- Disaster Recovery
- Cyber Continuity of Government (COOP)

Objective #2: Develop a Washington State Cyber Incident Response Plan

CEMP designed as an "All Hazards" Emergency Management Plan

- Domestic cyber issues are "All Hazard" along with other natural and manmade disasters
- **Current plan mentions "cyber" <u>twice</u> in 119 pages**



Washington State

Comprehensive Emergency Management Plan

- Basic Plan -

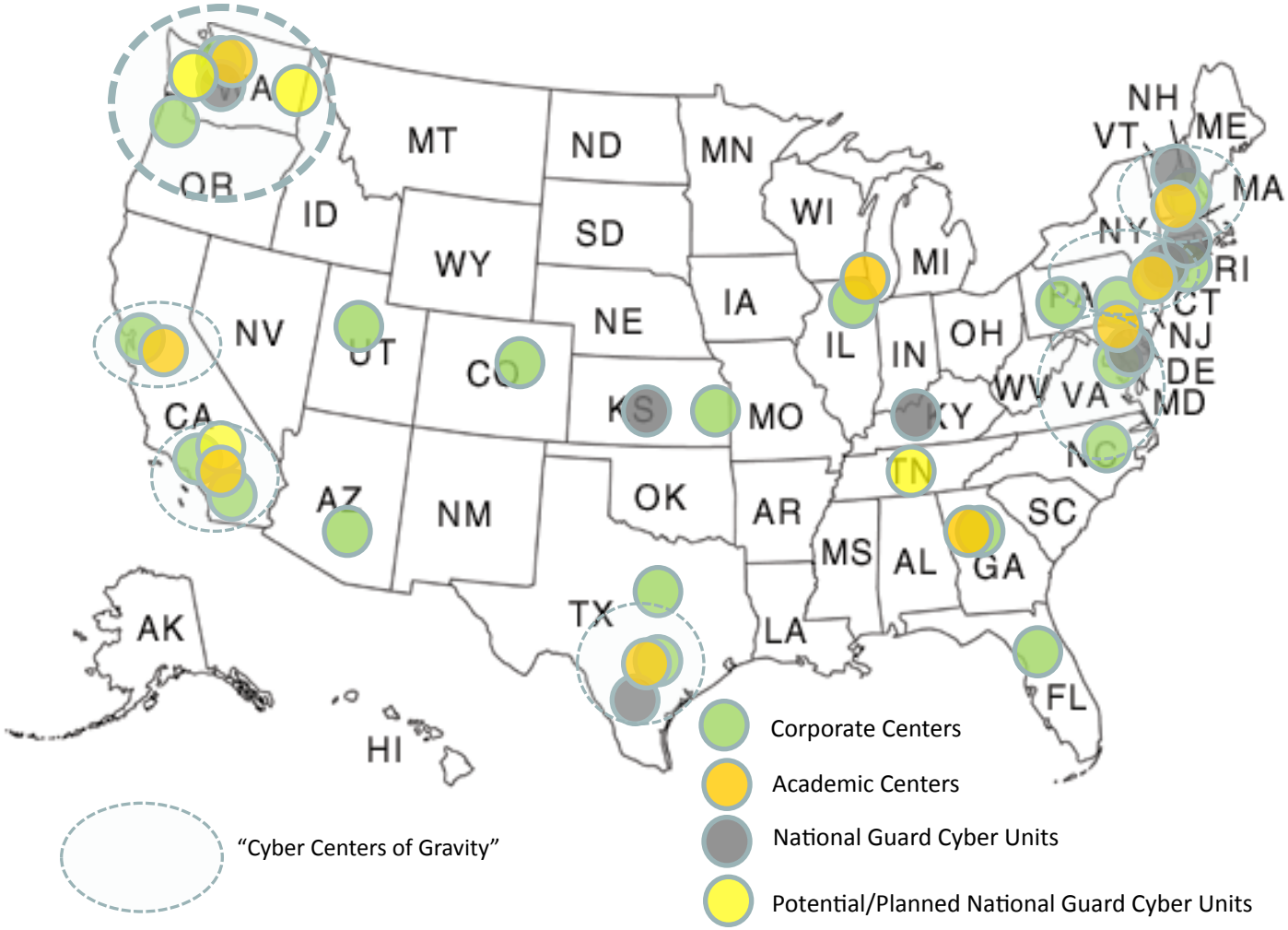
June 2011

Washington State Military Department
Emergency Management Division

Objective #3: Cyber Center of Excellence

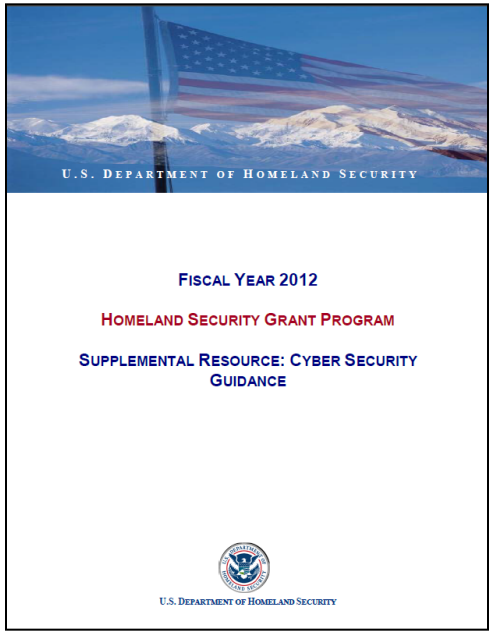
Leverage WA State efforts for others in FEMA Region X and nationally

- **Completes the "Cyber Center of Excellence" in the Pacific Northwest**

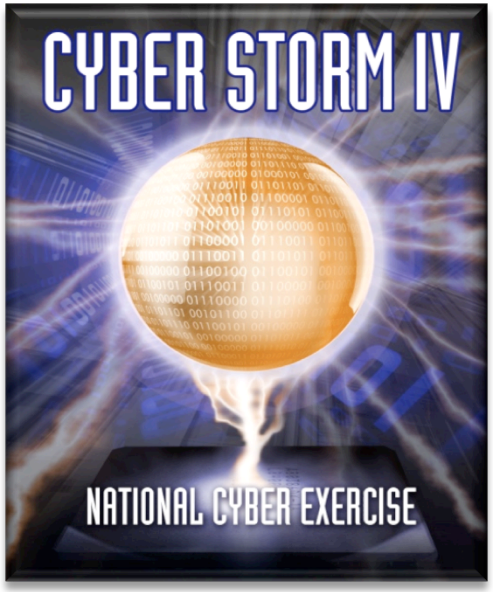


Accomplishments to date

- **FY12 DHS HLS Grant – $80k to OCIO for domestic cyber planning**
  - $40k matching funds to hire state Cyber Policy Coordinator
  - $25k for National Guard penetration testing of cyber critical infrastructure (in State Active Duty)
  - $15k to begin development of state-wide cyber critical infrastructure response plan



- **DHS Cyberstorm IV exercise (14-15 Aug)**
  - Hosted by WA Consolidated Technology Services
  - Opportunity to validate Washington National Guard cyber support Conops
  - Capture issues/gaps for potential FY13 DHS grant funding



Summary

- Washington Military Department is exercising a ground-breaking leadership role in bottom-up State Cyber planning efforts
- Partnerships with other State agencies and private sector critical infrastructure owners / operators is critical for success
- Need to develop capabilities locally and leverage them nationally
- Already realizing benefits from these initial State IPT initiatives

Thank You

Adam Wehrenberg
RCPGP Project Director
City of Boston OEM
617-635-3429
adam.wehrenberg@cityofboston.gov

Theresa Murray
Executive Director
Rhode Island Emergency Management Agency
401-946-9996
theresa.c.murray@us.army.mil

Gent Welsh, Lt Col, WA ANG
Chief Information Officer/J6
Washington Military Department
253-512-7575
gent.welsh@ang.af.mil

Robert Fitzpatrick
Regional Catastrophic Planner
Rhode Island Emergency Management Agency
401-462-7142
robert.j.fitzpatrick.ctr@us.army.mil

NERCPI